

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-022647
 (43)Date of publication of application : 26.01.2001

(51)Int.Cl. G06F 12/14
 G06F 15/00
 G09C 1/00
 G11B 20/10
 H04L 9/32

(21)Application number : 11-196207

(71)Applicant : TOSHIBA CORP
 MATSUSHITA ELECTRIC IND CO
 LTD

(22)Date of filing : 09.07.1999

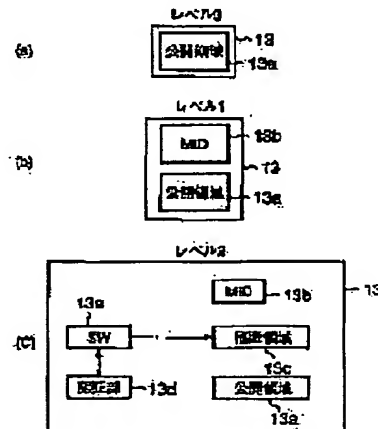
(72)Inventor : KAMIBAYASHI TATSU
 KATO HIROSHI
 TOMA HIDEYUKI
 TATEBAYASHI MAKOTO
 HARADA TOSHIHARU
 YAMADA HISASHI

(54) METHOD AND DEVICE FOR CONTENTS MANAGEMENT, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To securely and safely erase contents recorded on a recording medium by decoding and comparing data, used for overwriting on an opposite side, with overwriting data when the data are transferred and confirming that necessary information has been erased when recorded contents are deciphered.

SOLUTION: Overwriting data for erasing information, needed to decipher contents recorded on a recording medium (MC) 13, by overwriting are deciphered by using 1st common information generated by mutual authentication and then transferred to an opposite side. When data used for overwriting on the opposite side are transferred from the opposite side after being ciphered by using 2nd common information generated by performing mutual authentication again, the data are deciphered with the 2nd common information and then compared with the overwriting data to confirm that the information needed to decipher the recorded contents has been erased. Where, the MC 13 processes an open area 13a, an identification information storage 13b, a secrecy 13c and an authentication part 13d, etc.



LEGAL STATUS

[Date of request for examination] 19.10.2004
 [Date of sending the examiner's decision of rejection]

BEST AVAILABLE COPY

(2) 特開2001-22647

【特許請求の範囲】

【請求項1】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第1の共有情報を用いて暗号化してから相手側に転送し、前記相手側から、再度の相互認証により生成された第2の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたとき、それを前記第2の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認することを特徴とするコンテンツ管理方法。

【請求項2】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報が相互認証により生成された共有情報を用いて暗号化されて相手側から転送された後、再度相互に認証されたとき、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去することを特徴とするコンテンツ管理方法。

【請求項3】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第1の共有情報を用いて暗号化してから相手側に転送する転送手段と、前記相手側から、再度の相互認証により生成された第2の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたとき、それを前記第2の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認する確認手段と、を具備したことを特徴とするコンテンツ管理装置。

【請求項4】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相互認証により生成された共有情報を用いて相手側に転送する転送手段と、この転送手段で指示情報を転送した後、再度相互に認証を行って、前記記録媒体に記録されたコンテンツを復号する際に必要な情報の消去を前記相手側に行わせる消去実行手段と、を具備したことを特徴とするコンテンツ管理装置。

【請求項5】 演算処理機能を有する記録媒体であって、相互認証により生成された第1の共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に

必要な情報を上書きすることにより消去するための上書きデータを相手側より受信したとき、前記第1の共有情報を用いて復号して得られたデータを用いて自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去する消去手段と、

この消去手段で上書きに用いたデータを再度の相互認証により生成された第2の共有情報を用いて暗号化して前記相手側に転送する転送手段と、を具備したことを特徴とする記録媒体。

【請求項6】 演算処理機能を有する記録媒体であって、相互認証により生成された共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相手側より受信した後、再度相互に認証されたとき、自己に記録されたコンテンツを復号する際に必要な情報を消去する手段を具備したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理方法およびそれを用いたコンテンツ管理装置に関し、特に、記録媒体に記録された複製コンテンツの消去方法に関する。

【0002】

【従来の技術】従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【0003】さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと対照的に、移動は、異なった場所（記録媒体（メディア））にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【0004】

【発明が解決しようとする課題】近年、ネットワーク等を通じたオリジナルに忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的の（移動による）配布は、著作権管理を行うことができない。

【0005】このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【0006】特に、著作権保護のため、複製コンテンツの数を規制しながら記録媒体に対し複製コンテンツの記録および消去を行うコンテンツ管理においては、記録媒体に記録された複製コンテンツの移動の際に、当該記録

(3)

特開2001-22647

3

媒体に記録されている複製コンテンツを確実に消去する必要がある。この場合、複製コンテンツの記録を行う場合とは異なり、その手続の際に、第三者が不正に、例えば複製コンテンツの消去のためのコマンド等を受け取らないよう信号をカット等することにより、容易に当該記録媒体から複製コンテンツの消去を回避することができ

る。
【0007】そこで、本発明は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理において、記録媒体に記録されたコンテンツの消去が確実にし

かも安全に行えるコンテンツ管理方法およびそれを用いたコンテンツ管理装置および記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】(1) 本発明のコンテンツ管理方法(請求項1)は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第1の共有情報を用いて暗号化してから相手側に転送し、前記相手側から、再度の相互認証により生成された第2の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたら、それを前記第2の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認することを特徴とする。

【0009】また、本発明のコンテンツ管理装置(請求項3)は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第1の共有情報を用いて暗号化してから相手側に転送する転送手段と、前記相手側から、再度の相互認証により生成された第2の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたら、それを前記第2の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認する確認手段とを具備したことを特徴とする。

【0010】本発明の記録媒体(請求項5)は、演算処理機能を有する記録媒体であって、相互認証により生成された第1の共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相手側より受信したとき、前記第1の共有情報を用いて復号して得られたデータを用いて自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去する消去手段と、この消去手段で上書きに用いたデータを

4

再度の相互認証により生成された第2の共有情報を用いて暗号化して前記相手側に転送する転送手段とを具備したことを特徴とする。

【0011】上記本発明によれば、例えば、第三者によるコンテンツの消去のためのコマンド等を受け取らないようにする攻撃を確実に回避することができ、記録媒体に記録されたコンテンツの消去が確実にしかも安全に行え、記録媒体に記録するコンテンツの数の管理が容易にしかも確実に行える。

10 【0012】(2) 本発明のコンテンツ管理方法(請求項2)は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報が相互認証により生成された共有情報を用いて暗号化されて相手側から転送された後、再度相互に認証されたとき、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去することを特徴とする。

20 【0013】本発明のコンテンツ管理装置(請求項4)は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相互認証により生成された共有情報を用いて相手側に転送する転送手段と、この転送手段で指示情報を転送した後、再度相互に認証を行って、前記記録媒体に記録されたコンテンツを復号する際に必要な情報の消去を前記相手側に行行させる消去実行手段とを具備したことを特徴とする。

30 【0014】本発明の記録媒体(請求項6)は、演算処理機能を有する記録媒体であって、相互認証により生成された共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相手側より受信した後、再度相互に認証されたとき、自己に記録されたコンテンツを復号する際に必要な情報を消去する手段を具備したことを特徴とする。

40 【0015】上記本発明によれば、例えば、第三者によるコンテンツの消去のためのコマンド等を受け取らないようにする攻撃を確実に回避することができ、記録媒体に記録されたコンテンツの消去が確実にしかも安全に行え、記録媒体に記録するコンテンツの数の管理が容易にしかも確実に行える。

【0016】

【発明の実施の形態】以下、本発明の一実施形態について図面を参照して説明する。

50 【0017】図1は、本実施形態にかかる記録媒体(メディア)に記録できる複製コンテンツの数を規制し、メディアへの複製コンテンツの記録、メディアに記録された複製コンテンツの再生等を行う音楽コンテンツ利用管理システム(以下、簡単にLCMと呼ぶことがある)1

5

の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らず、映画や、ゲームソフト等であってもよい。また、メディアとしてメモ리카ード(MC)を用いているが、この場合に限るものではなく、フロッピーディスク、DVD等の各種記録媒体であってもよい。

【0018】EMD(Electronic Music Distributor)は、音楽配信サーバまたは音楽配信放送局である。

【0019】コンテンツ利用管理システム1は、例えば、パソコン(PC)であり、複数のEMD(ここでは、EMD#1～#3)に対応した受信部#1～#3を具備しており、EMDが配信する暗号化コンテンツまたはそのライセンス(利用条件と暗号化コンテンツの復号鍵Kc)などを受信する。受信部#1～#3は、再生機能や課金機能を有していても良い。配信された音楽コンテンツを試聴する為に再生機能が利用される。又、課金機能を利用して、気に入ったコンテンツを購入する事が可能である。

【0020】LCM1は、セキュア・コンテンツ・サーバ(ここでは、Secure Music Server: SMSで、以下、簡単にSMSと呼ぶことがある)2を具備し、利用者が購入したコンテンツはEMDインタフェース(I/F)部3を経由してSMS2に送信される。音楽コンテンツは、必要に応じてEMD1/P部3で復号され、形式変換や再暗号化が施される。SMS2が暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵をライセンス格納部9に格納する。SMS2が再生機能を有していても良い。当該再生機能により、SMS2が管理する音楽コンテンツをPC上で再生する事ができる。

【0021】SMS2は、メディア(以下、簡単にMC(memory card)と呼ぶことがある)13に対してコンテンツデータを出力する機能を有している。MC13を記録再生装置(以下、簡単にPD(Portable Device)と呼ぶことがある)12にセットし、MC13に記録されたコンテンツを再生することができる。

【0022】SMS2からMC13へのコンテンツの記録はメディア(MC)インタフェース(I/F)部6を通じて直接行われるか、又はPD12を経由して行うことができる。

【0023】デバイスID格納部4は、例えば、ROMで構成され、当該LCMの識別情報(デバイスID)が格納されている。

【0024】MC13は、そのメディア固有かつ書き換え不能の識別情報(MID)を有しており、MC13に格納されるコンテンツは、MC13に依存する暗号化鍵で暗号化されていてもよい。

【0025】まず、チェックイン/チェックアウトについて、図1のLCM1に則して説明する。

【0026】チェックアウトとは、LCM1が「親」と

[4]

特開2001-22647

6

してのコンテンツを格納しており、MC13に、その複製を「子」コンテンツとしてコピーすることをいう。

「子」コンテンツはPD12で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、MC13をLCM1に接続し、LCM1が「子」コンテンツを消去(又は利用不能)する事で、LCM1内の「親」コンテンツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0027】このチェックイン/チェックアウトを単純に、従来からのLCM1で実現しようとすると、実際の様な「攻撃」が存在する。すなわち、MC13に格納された「子」を別の記憶メディアに(MIDを除いて)退避しておき、MC13の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該MC13に書き戻す。既にチェックインは済んでいるので、LCM1上の「親」は別のMC13に「子」をコピーして良い。この方法で、任意の回数だけ利用可能な「子」を作る事が可能である。

【0028】上述の「攻撃」には、MC13とLCM1とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、MC13は正当なLCM1以外からのデータ転送を受け付けず、LCM1が正当なMC13以外からのデータ転送を受け付けないと仮定する。この場合、MC13内の「子」を別の記憶メディアに退避する事はできない。又、LCM1に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。

【0029】ところが、実は、LCM1とMC13との認証を前提としても、チェックイン/チェックアウトは実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、LCM1上の「親」が「子」を作っていない状態で、LCM1のデータ(特に、ライセンス格納部9の情報)を別の記憶メディアにバックアップする。MC13に「子」をコピーした後、バックアップしたLCM1のデータを復元する。LCM1の「親」は「子」を作る前の状態に戻るから、別のMC13に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。

【0030】そこで、このような攻撃にも対処できるチェックイン/チェックアウトを実現するために、MC13内の記憶領域に、公開された手順では読み書きできない領域(秘密領域)を設け、そこに相互認証に必要な情報やコンテンツ復号に必要な情報や、アクセス不可能であるデバイス(LCM1、PD12)の識別情報(デバイスID)のリスト(リボケーションリスト(RVCリスト))等を記録する(図2参照)。また、LCM1の記憶領域(例えば、LCM1がPCで構成されている場

(5) 特開2001-22647

7

合には、ハードディスク（HDD）上に非公開の手順でしかアクセスできない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図2参照）。さらに、PD12の記憶領域上に非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図2参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【0031】図1に示すように、LCM1では、秘匿領域には、宿帳格納部8が設けられ、SMS2にてこの宿帳格納部8にアクセスするための秘匿された特定の手続が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ7を具備している。

【0032】図4（c）に示すように、MC13は、その識別情報MIDを格納するための外部からは書き換え不可能で、コピーも不可能なような構成になっている識別情報格納部（ROM）13bと、秘匿領域13cと、公開領域（読み書き可能なRAM）13aと、秘匿領域13cがアクセスされる際に認証部13dにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域13cにアクセス可能なようにゲートを開くスイッチ（SW）13eを具備する。

【0033】なお、本実施形態で利用可能なMC13は、3種類あり、図4（c）に示すような、識別情報MIDと秘匿領域とを両方兼ね備えているMC13の種別を「レベル2」と呼ぶ。秘匿領域を持たない識別情報MIDは持つ図4（b）に示すようなMC13の種別を「レベル1」と呼ぶ。秘匿領域も識別情報も持たない図4（a）に示すような公開領域だけのMC13の種別を「レベル0」と呼ぶことにする。これら種別は、例えば、識別情報MIDの有無でレベル0とそれ以外の種別とが判別でき、さらに、識別情報MIDの構成からレベル1とレベル2とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル2であるとする。

【0034】以下、特に断らない限り、レベル2のMC13の場合を例にとり説明する。

【0035】このMC13は、LCM1に接続されたPD12にセットして用いる場合とLCM1に直接セットして用いる場合とがある。

【0036】図3は、PD12の構成例を示したもので、MC13は、メディアインタフェース（I/F部）12fにセットされる。LCM1がPD12を介してMC13に読み書きする場合は、PD12内の秘匿領域アクセス部を経由してMC13の秘匿領域にアクセスする。メディアI/F部12fには、MC13の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。PD12内の秘匿領域は、フラッシュメモリ12dに設けられていてもよい。ROM12cには、MC1

8

3、LCM1との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証手続を記述したプログラムや、MC13の種別を判別するためのプログラムも書き込まれていて、このプログラムに従って、CPU12aの制御の下、MC13との間の各種認証、種別判別等の処理を実行するようになっている。

【0037】ROM12cには、PD12の識別情報（デバイスID）が格納されていてもよい。また、例えば、フラッシュメモリ12dに設けられた秘匿領域に秘匿デバイスID（SPDID）が予め格納されている。

【0038】図5は、LCM1のメディアI/F部6の構成を示したもので、MC13との間で相互認証を行うための認証部6cと、MC13の種別を判別するメディア判別部6bと、これら全体を制御するための制御部6aとから構成されている。認証部6cは、MC13の秘匿領域にアクセスするための秘匿領域アクセス部でもある。

【0039】図24は、図4（c）に示したレベル2のMC13の構成をより具体的に示したものである。図24に示すように、秘匿領域102は、例えば、1チップのメモリ素子（例えばRAM）上に構成され、RAM領域とROM領域とを有している。例えば、RAM領域であるかROM領域であるかは例えばCPU等から構成される制御部101によるアクセス制御の違いにより区別する。公開領域にはROM領域103とRAM領域104とがそれぞれ別個のメモリ素子で構成されている。

【0040】制御部101には、秘匿領域102へアクセスする際と公開領域103、104へアクセスする際とでそれぞれ別個のバスが接続されていて、制御部101は、いずれか一方のバスに切り替えて秘匿領域102、あるいは公開領域103、104へアクセスするようになっている。

【0041】制御部101は、MC13の各構成部の制御を司さるとともに、LCM1等がMC13の秘匿領域にアクセスする度に行われる認証処理（AKE）も実行する。

【0042】秘匿領域102中のROM領域には、例えば、MC13、LCM1との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証処理（AKE）を記述したプログラムや、秘匿メディアID（SMID）等が予め格納されていてもよい。

【0043】次に、LCM1の秘匿領域に格納される宿帳について説明する。

【0044】SMS2にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツID（TID）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部8に図7（a）に示すような形態で記録されている。

(6) 特開2001-22647

9

【0045】図7(a)において、例えば、コンテンツID「TID1」なる子の残数は「2」で、そのチェックアウトリストはL1である。

【0046】チェックアウトリストは、複製コンテンツ(子)を記録したMC13の識別情報のリストであって、例えば、図7(a)において、チェックアウトリストL1には「m1」と「m2」という識別情報を持つ2つのMC13にコンテンツID「TID1」なるコンテンツの子がチェックアウトされていることがわかる。

【0047】以下、次に示す項目の順に説明する。

【0048】(1) 相互認証方法の概略

(2) レベル2のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

(3) レベル0のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

(1) 相互認証方法の概略

前述したように、チェックイン/チェックアウトを安全に行うために、LCM1、PD12とMC13との間で

(例えば、互いに同じアルゴリズムをもっているかの確認のための)相互認証を行う必要がある。一般に、相互認証処理には、相互認証を行う一方と他方とで共有する秘密の情報を保持する必要がある。従って、このような秘密情報を例えばMC13とLCM1およびPD12が持つことになる。情報セキュリティの観点から考えると、この秘密情報は、認証を行う度に毎回異なるものが生成されるといった動的なものであった方がよい。しかし、MC13というメディア自体にそのような秘密情報を生成するための高度な機能を追加すると、メディアが高価になってしまう。メディアを広く一般大衆に普及させるためには、できるだけ安価である方が望ましい。従って、メディア(MC13)のコスト低減化を考えれば、秘密情報をMC13に予め記憶させておく方がよい。

【0049】しかし、全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報(以下、このような情報をグローバルシークレットな情報と呼ぶ)を各メディアに予め記憶させた場合、ある1つのメディアからその秘密情報が何らかの方法により読まれてしまったとき、同じ秘密情報を記憶する他のメディアも不正に利用されてしまうという問題点があった。メディアにグローバルシークレットな情報を持たせることは極めて危険である(図8(a)参照)。

【0050】ある1つのメディアに記憶されている秘密情報が不当に読まれてしまっても、不正に使用できるのは、その秘密情報が読まれたメディアだけであれば問題がないわけであるから、秘密情報は、個々のメディアに固有のものであればよい。

【0051】そこで、ここでは、個々のメディアにメディア毎にそれぞれ異なる相互認証のための秘密情報を記憶させておき、この情報を用いてLCM1あるいはPD12とMC13とが相互認証を行うことにより、低コス

10

トなメディアを用いた、よりセキュリティ性の高い安全な相互認証方法を提案する。すなわち、本実施形態で説明する相互認証方法は、図8(b)に示すように、個々のメディア(レベル2のメディア)に相互認証(AKE)のために必要な各メディア毎にそれぞれ異なる秘密情報(ここでは、秘密メディアID(SMID))で、これは、メディアIDを何らかの方法で取得した暗号情報KMで予め暗号化されたものを(秘密領域に)予め記憶させておき、LCM1、PD12には、そのメディアの識別情報(MID)を転送する。LCM1あるいはPD12側では、MIDと、先に何らかの方法で取得した情報(KM)とを用いて相互認証のための情報(メディアのもつSMIDと同じもの)を所定のアルゴリズムを用いて生成して認証処理(AKE)を行う。

【0052】このように、MC13にはそれぞれに固有の秘密情報(SMID)を持たせておくだけで、LCM1、PD12がメディアから転送されてきた各メディア毎に固有の情報(MID)を基に秘密情報(SMID)を生成することにより、メディアに負荷をかけずに安全な相互認証が行える。

【0053】なお、以下の説明において、上記した相互認証処理をAKEと呼ぶことにする。

【0054】MC13がLCM1のメディアI/F部6、あるいは、PD12にセットされると、まず、メディアI/F部6とMC13との間、あるいは、PD12とMC13との間で相互認証が行われてもよい(図9のステップS1)。そして、双方にて正当な(例えば、同じ規格のハードウェア構成である)相手であると判断されたとき(ステップS2)、メディアI/F部6あるいはPD12はMC13から読み取った識別情報MIDを基に、MC13の種別を判別する(ステップS3)。そして、メディアI/F部6あるいはPD12は、その種別に応じたチェックイン/チェックアウト/再生処理を実行する(ステップS6)。

【0055】なお、図9のステップS1における相互認証は、必ずしも図8(b)に示したような相互認証である必要はない。

【0056】また、MC13にはレベル0からレベル2までの3種類があると説明したが、ここでは、レベル0とレベル2の2種類のMC13を対象として、図9以降の複製コンテンツのチェックイン/チェックアウト/再生処理動作について説明する。

【0057】さらに、以下の説明では、省略しているが、LCM1とMC13との間、LCM1とPD12との間、PD12とMC13との間で、それぞれの秘密領域にアクセスする際には、一方と他方との間で相互認証を行い、双方の正当性が確認されたらそれぞれの秘密領域へのゲートを開き、秘密領域へのアクセスが終了したら秘密領域へのアクセスを可能にしていたゲートを閉じる仕組みになっているものとする。例えば、LCM1と

(7)

特開2001-22647

11

12

MC13との間において、SMS2は、MC13の秘密領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘密領域13cへのゲートが開かれると、秘密領域13c内に鍵情報等を若込み、それが終了すると秘密領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。

【0058】(2) レベル2のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

図4(c)に示したような構成のレベル2のMC13を用いたチェックイン/チェックアウト、再生処理動作について説明する。

【0059】チェックアウトの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合)、SMS2に対しなされた場合について、図10を参照して説明する。

【0060】SMS2は、複製のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数nを調べ、 $n > 0$ のとき、デバイスID格納部4から当該LCM1のデバイスID(LCMID)を読み出し、それをMC13へ転送する(ステップS101)。

【0061】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS102)、登録されていないとき秘密領域13cにアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS103)。MC13は、さらに、識別情報格納部13bから、その識別情報(MID)を読み出して同じくLCM1へ転送する(ステップS104)。

【0062】LCM1では、MC13から転送されてきたメディアID(MID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[MID])を生成する(ステップS105)。

【0063】LCM1では、この生成された情報KM[MID]を用いて相互認証処理(AKE)を実行し、一方、MC13でも秘密メディアID(SMID)を用いて相互認証処理(AKE)を実行する(ステップS106)。この相互認証処理(AKE)では、LCM1とMC13とが同じ関数 $g(x, y)$ 、 $H(x, y)$ を共有していて、LCM1で生成された情報KM[MID]が当該MC13の秘密メディアID(SMID)と同じであるならば、相互認証処理(AKE)により互に一方が他方を正当であると確認できるようになっている。

【0064】ここで、図22を参照して、ステップS106の相互認証処理(AKE)の処理動作について説明する。

【0065】LCM1は、乱数R1を発生し(ステップ

S301)して、それをMC13に転送するとともに、2つの変数 x, y を有する関数 $g(x, y)$ の一方の変数に代入する。また、図10のステップS105で生成された情報KM[MID]を関数 $g(x, y)$ の他方の変数に代入して、関数 g の値を求める(ステップS302)。

【0066】一方、MC13でも、LCM1から転送されてきた乱数R1を関数 $g(x, y)$ の一方の変数に代入し、自身の秘密メディアID(SMID)を他方の変数に代入して、求めた関数 g の値をLCM1へ転送する(ステップS303)。

【0067】LCM1では、MC13から転送されてきた関数 g の値と、LCM1側で求めた関数 g の値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、LCM1側でのAKEの処理を中止する(ステップS304)。

【0068】次に、MC13では、乱数R2を発生し(ステップS305)して、それをLCM1に転送するとともに、2つの変数を有する関数 $g(x, y)$ の一方の変数に代入する。また、当該MC13の秘密メディアID(SMID)を関数 $g(x, y)$ の他方の変数に代入して、関数 g の値を求める(ステップS306)。

【0069】一方、LCM1でも、MC13から転送されてきた乱数R2を関数 $g(x, y)$ の一方の変数に代入し、また、図10のステップS105で生成された情報KM[MID]を関数 $g(x, y)$ の他方の変数に代入して、関数 g の値を求めたら、それをMC13へ転送する(ステップS307)。

【0070】MC13では、LCM1から転送されてきた関数 g の値と、MC13側で求めた関数 g の値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、MC13側でのAKEの処理を中止する(ステップS308)。

【0071】MC13では、ステップS308で、関数 g の値が一致していたら、2つの変数を有する関数 $H(x, y)$ の一方の変数に乱数R2、他方の変数に当該MC13の秘密メディアID(SMID)を代入して鍵情報KTを生成する(ステップS309)。

【0072】一方、LCM1でも、ステップS304で関数 g の値が一致していたら、MC13から転送されてきた乱数R2を関数 $H(x, y)$ の一方の変数に代入するとともに、図10のステップS105で生成された情報KM[MID]を他方の変数に代入して鍵情報KTを生成する(ステップS310)。

【0073】なお、ステップS304、ステップS308のそれぞれで関数 g の値が一致したことによりLCM1とMC13のそれぞれで同じ関数 $H(x, y)$ を用いて生成される鍵情報KTは同じものである。LCM1とMC13のそれぞれでは、以降、この鍵情報KTを用いてコンテンツ復号鍵Kcの受け渡しを行うようになって

13

いる。

【0074】また、相互認証処理(AKE)で生成される鍵情報KTは、毎回異なるものである方が情報セキュリティ上望ましい。ここでは、鍵情報KTを生成する関数Hに代入される2つの変数のうちの一方には、毎回新たに生成される乱数R2が代入されるので、毎回異なる鍵情報KTが生成される。

【0075】図10の説明に戻り、ステップS106において、LCM1とMC13との間で相互に認証されたときは、MC13では、生成した鍵情報KT(ここでは、KT1とする)を秘密領域に格納する(ステップS107)。また、LCM1では、暗号化コンテンツを復号するための復号鍵(コンテンツ復号鍵)KcをステップS106で生成された鍵情報KT1で暗号化して(KT1[Kc])MC13へ転送し(ステップS108～ステップS109)、コンテンツ情報CをKcで暗号化して(Kc[C])MC13へ転送する(ステップS110～ステップS111)。

【0076】最後に、SMS2は、図7(b)に示すように、宿機のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数nから「1」減算し、チェックアウトリストL1に、当該MC13の識別情報「m0」を追加する。

【0077】MC13は、転送されてきた暗号化されたコンテンツ復号鍵KT1[Kc]、暗号化コンテンツKc[C]を公開領域13aに格納する。

【0078】以上の処理が終了したときのMC13の記憶内容を図6に示す。

【0079】次に、再生の指示がLCM1のユーザインタフェース(I/F)部15を介してSMS2に、あるいは、PD12に対しなされた場合について、図11を参照して説明する。

【0080】まず、PD12あるいはLCM1は、自身のデバイスIDをMC13へ転送する(ステップS121)。

【0081】LCM1が図3に示すようなPD2のコンテンツの再生機能部(復調部12g、デコード12h、D/A変換部12i等)を持っているのであれば、MC13をPD12で再生する場合もLCM1で再生する場合も同様であるので、以下、PD12で再生する場合を例にとり説明する。

【0082】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS122)、登録されていないとき秘密領域13cにアクセスしてマスターキーKMを読み出して、PD12へ転送する(ステップS123)。MC13は、さらに、識別情報格納部13bから、その識別情報(MID)を読み出して同じくPD12へ転送する(ステップS124)。

【0083】PD12では、MC13から転送されてき

(8)

特開2001-22647

14

たメディアID(MID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[MID])を生成する(ステップS125)。

【0084】PD12では、この生成された情報KM[MID]を用いて相互認証処理(AKE)を実行し、一方、MC13でも秘密メディアID(SMID)を用いて相互認証処理(AKE)を実行する(ステップS126)。ステップS126の相互認証処理(AKE)は、図22と同様であるので説明は省略する。

【0085】PD12とMC13との間で相互に認証されたときは、MC13では、生成した鍵情報KT(ここでは、KT2とする)を用いて秘密領域13cに格納されていた鍵情報KT1を暗号化して(KT2[KT1])、PD12へ転送する(ステップS127～ステップS128)。一方、PD12では、ステップS126で生成された鍵情報KT2を用いてMC13から転送されてきたKT2[KT1]を復号することができる(ステップS128)。

【0086】MC13からは暗号化されたコンテンツ復号鍵KT1[Kc]、暗号化コンテンツKc[C]を公開領域13aから読み出してPD12へ転送する(ステップS129、ステップS131)。

【0087】PD12は、鍵情報KT1の復号に成功していれば、それを用いて暗号化されたコンテンツ復号鍵KT1[Kc]を復号してコンテンツ復号鍵Kcが得られるので(ステップS130)、このコンテンツ復号鍵Kcを用いて暗号化コンテンツKc[C]を復号して、コンテンツCを得る(ステップS132)。そして、PD12では、コンテンツCをデコード12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

【0088】次に、チェックインの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合)、SMS2になされた場合について、図12を参照して説明する。

【0089】図12に示すチェックイン時の処理動作は、MC13に記録した鍵情報(あるいは鍵情報と暗号化コンテンツ情報)を消去(乱数で上書き消去)する際と、消去されたことの確認を行う際との合計2回、相互認証処理(AKE)を行うものである。

【0090】SMS2は、デバイスID格納部4から当該LCM1のデバイスID(LCMID)を読み出し、それをMC13へ転送する(ステップS141)。

【0091】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS142)、登録されていないとき秘密領域13cにアクセスしてマスターキーKMを読み出して、LC

(9) 時間 2001-22647

15

M1へ転送する(ステップS143)。MC13は、さらに、識別情報格納部13bから、その識別情報(MID)を読み出して同じくLCM1へ転送する(ステップS144)。

【0092】LCM1では、MC13から転送されてきたメディアID(MID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[MID])を生成する(ステップS145)。

【0093】LCM1では、この生成された情報KM[MID]を用いて第1の相互認証処理(AKE#1)を実行し、一方、MC13でも秘密メディアID(SMID)を用いて第1の相互認証処理(AKE#1)を実行する(ステップS146)。

【0094】ステップS146の相互認証処理(AKE#1)は、図22と同様であるので説明は省略する。

【0095】ステップS146において、LCM1とMC13との間で相互に認証されたときは、LCM1では、MC13の秘密領域(RAM領域)13cに格納されている鍵情報KT1を上書きするための乱数r1を従来からある乱数発生器を用いて発生して、それとMC13への上書き指示情報とをステップS146で生成した鍵情報KT(ここではKT3とする)で暗号化して(KT3[上書き指示+r1])MC13へ転送する(ステップS501)。なお、上書き指示には、鍵情報KT1の書き込まれているアドレスが含まれていてもよい。

【0096】MC13では、LCM1から転送されてきたKT3[上書き指示+r1]をステップS146で生成した鍵情報KT3で復号し、乱数r1を得る(ステップS502)。この乱数r1で、MC13の秘密領域(RAM領域)13cに格納されている鍵情報KT1を上書きすることで消去する(ステップS503)。なお、鍵情報KT1の他に、さらにコンテンツ復号鍵Kcを鍵情報KT1で暗号化したもの(KT1[Kc])や暗号化コンテンツ情報Kc[C]も乱数r1で上書きすることで消去してもよい。

【0097】次に、鍵情報KT1(あるいは、鍵情報KT1と暗号化コンテンツ情報等)が乱数r1にて確実に消去されたか否かの確認のための処理を実行する。すなわち、LCM1では、ステップS145で生成された情報KM[MID]を用いて第2の相互認証処理(AKE#2)を実行し、一方、MC13でも秘密メディアID(SMID)を用いて第2の相互認証処理(AKE#2)を実行する(ステップS504)。

【0098】ステップS504の第2の相互認証処理(AKE#2)は、図22と同様であるので説明は省略する。

【0099】ステップS504において、LCM1とMC13との間で相互に認証されたときは、MC13は、鍵情報KT1(あるいは、鍵情報KT1と暗号化コンテンツ情報等)が格納されていたアドレスからデータ(正

16

常に上書きされていれば、乱数r1)を読み取って、それをステップS504で生成された鍵情報KT(ここではKT4とする)で暗号化して(KT4[r1])LCM1へ転送する(ステップS505)。

【0100】LCM1では、MC13から転送されてきたKT4[r1]をステップS504で生成した鍵情報KT4で復号し(ステップS506)、その際得られたデータとステップS501で発生した乱数r1とを比較し、一致していれば、MC13において、鍵情報KT1(あるいは、鍵情報KT1と暗号化コンテンツ情報等)が乱数r1にて消去されたと判断し、処理を終了する(ステップS507)。不一致のときはLCM1は異常を通知する等の処置を講ずるのが望ましい。

【0101】最後に、図7(c)に示すように、宿根のチェックイン要求のあったコンテンツID「TID1」のコンテンツの予の残数nに「1」加算し、チェックアウトリストL1から、当該MC13の識別情報m0を削除する。

【0102】次に、図12とは異なる他のチェックイン時の処理動作について、図13を参照して説明する。なお、図12と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図13に示すチェックイン時の処理動作は、MC13に記録した鍵情報(あるいは鍵情報と暗号化コンテンツ情報)を消去するための指示情報(例えば、これからチェックインを行う旨の指示情報)の転送の際と、実際に消去するためのコマンド発生トリガとしての合計2回、相互認証処理(AKE)を行う点に特徴があり、ステップS146のAKE#1までの処理動作は図12と同様である。

【0103】ステップS146において、LCM1とMC13との間で相互に認証されたときは、LCM1では、これからチェックインを行う旨の指示情報をステップS146で生成した鍵情報KT(ここではKT3とする)で暗号化して(KT3[チェックイン指示])MC13へ転送する(ステップS551)。なお、チェックイン指示には、鍵情報KT1の書き込まれているアドレスが含まれていてもよい。

【0104】MC13では、LCM1から転送されてきたKT3[チェックイン指示]をステップS146で生成した鍵情報KT3で復号し、チェックイン指示情報を得る(ステップS552)。

【0105】次に、実際に消去するためのコマンド発生トリガとしての第2の相互認証処理(AKE#2)を実行する(ステップS553)。ここでのAKE#2は、図23に示すように、図22のステップS308と同様にして、関数gの値が一致していたか否かをチェックしたら、その結果を出力するのみである。

【0106】MC13では、関数gの値が一致していれば、かつ、先にチェックイン指示情報を得ていたときは、鍵情報KT1(あるいは、鍵情報KT1と暗号化コ

17

ンテンツ情報等)を消去する(ステップS554〜ステップS555)。例えば、MC13のファイル管理領域を書き換えることにより鍵情報KTI等を消去するようにしてもよい。

【0107】最後に、図7(c)に示すように、消滅のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該MC13の識別情報m0を削除する。

【0108】次に、図10とは異なる他のチェックアウト時の処理動作について、図14を参照して説明する。なお、図10と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図14では、MC13へ転送すべきコンテンツ復号鍵Kcに対する処理に特徴がある。

【0109】図14において、LCM1では、コンテンツ復号鍵Kcに対し、まず、ステップS105で生成されたKm[MID] (以下、これをwと表す)を用いて暗号化を施す(ステップS162)。そして、wで暗号化されたコンテンツ復号鍵Kc(w[Kc])をステップS106の相互認証処理(AKE)にて生成した鍵情報KTIを用いてさらに暗号化を行ってから(KTI[w[Kc]])、MC13へ転送する(ステップS163)。

【0110】MC13では、ステップS106の相互認証処理(AKE)にて生成した鍵情報KTIを用いて、転送されてきたKTI[w[Kc]]を復号してw[Kc]を得、これを秘密領域13へ格納する(ステップS164)。

【0111】コンテンツ情報Cは、図10の場合と同様に、Kcで暗号化してから(ステップS165)、MC13へ転送される(ステップS166)。

【0112】図14に示したようなチェックアウト処理動作に対応する再生処理動作について、図15を参照して説明する。なお、図11と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図15において、MC13は、秘密領域13cに格納されている暗号化コンテンツ復号鍵w[Kc]をステップS126の相互認証処理(AKE)で生成された鍵情報KT2で暗号化してから(KT2[w[Kc]])LCM1あるいはPD12へ転送する。(ステップS172)。LCM1あるいはPD12では、同じくステップS126で生成された鍵情報KT2でMC13から転送されてきたKT2[w[Kc]]を復号して(ステップS173)、その結果得られたw[Kc]をステップS123で生成されたw=KM[MID]を用いて復号して、コンテンツ復号鍵Kcを得る(ステップS174)。このコンテンツ復号鍵Kcを用いて暗号化コンテンツKc[C]を復号して、コンテンツCを得る(ステップS175)。そして、LCM1あるいはPD12では、コン

(10)

特開2001-22647

18

テンツCをデコーダ12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

【0113】図14に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図12、図13の説明とほぼ同様で、異なるのは、図12のステップS503、図13のステップS555でMC13の秘密領域13cから消去されるのは、鍵情報KTIではなく、w=KM[MID]で暗号化されたコンテンツ復号鍵w[Kc]であるという点である。

【0114】(3)レベル0のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生次に、図4(a)に示したような構成のレベル0のMC13を用いたチェックイン/チェックアウト、再生処理動作について説明する。

【0115】この場合、MC13は、PD12にセットされ、このPD12を介してLCM1との間でチェックアウト処理が実行される。基本的な動作は、MC13がレベル2の場合と同様であるが、レベル0の場合、秘密領域、メディアIDを有していないので、PD12がLCM1に対する処理をレベル0のMC13に代行して図10に示したような処理を実行することとなる。そのため、PD12の秘密領域には、マスターキーKM、秘密デバイスキーSPDID、リボケーションリスト(RVCRリスト)を予め記憶しておくものとする。なお、マスターキーKMは必ずしもメディアMC13に記憶しておくマスターキーKMとその機能は同じであるが、そのデータ自体は同じものである必要はない。

【0116】まず、図9のステップS3において、MC13の種別がレベル0であると判定される。

【0117】チェックアウトの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介してSMS2に与えられた場合について、図16を参照して説明する。

【0118】SMS2は、消滅のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数nを調べ、n>0のとき、デバイスID格納部4から当該LCM1のデバイスID(LCMID)を読み出し、それをPD12へ転送する(ステップS201)。

【0119】PD12では、転送されてきたデバイスIDがRVCRリストに登録されていないかチェックし(ステップS202)、登録されていないときPD12の秘密領域にアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS203)。PD12は、さらに、例えばROM12cからその識別情報、すなわち、デバイスID(PDID)を読み出して、同じくLCM1へ転送する(ステップS204)。

【0120】LCM1では、PD12から転送されてき

(11)

特開2001-22647

19

たデバイスID (PDID) をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM [PDID]) を生成する(ステップS205)。

【0121】LCM1では、この生成された情報KM [PDID] を用いて相互認証処理(AKE)を実行し、一方、PD12でも秘密デバイスID (SPDID) を用いて相互認証処理(AKE)を実行する(ステップS206)。ステップS206の相互認証処理(AKE)は、図22と同様であるので説明は省略する。

【0122】LCM1とPD12との間で相互に認証されたとき、PD12では、生成した鍵情報KT (ここでは、KT1とする) を秘密領域に格納する(ステップS207)。LCM1では、暗号化コンテンツを復号するための復号鍵(コンテンツ復号鍵) KcをステップS206で生成された鍵情報KT1で暗号化して(KT1 [Kc])、PD12を経由してMC13へ転送し(ステップS208～ステップS209)、また、コンテンツ情報CをKcで暗号化して(Kc [C])、PD12を経由してMC13へ転送する(ステップS210～ステップS211)。

【0123】最後に、SMS2は、図7(b)に示すように、宿根のチェックアウト要求のあったコンテンツID [TID1] のコンテンツの予の残数nから「1」減算し、チェックアウトリストL1に、当該PD12の識別情報PDIDを追加する。

【0124】MC13は、転送されてきた暗号化されたコンテンツ復号鍵KT1 [Kc]、暗号化コンテンツKc [C] を公開領域13aに格納する。

【0125】次に、再生の指示がPD12に対しなされた場合のPD12とMC13との間の処理動作について、図17を参照して説明する。

【0126】まず、MC13は、公開領域に記録されている暗号化されたコンテンツ復号鍵KT1 [Kc] をPD12へ転送する(ステップS221)。PD12が当該MC13に対し当該再生対象のコンテンツ情報をチェックアウトした際に用いたものであるならば、その秘密領域に暗号化されたコンテンツ復号鍵を復号するための鍵情報KT1を記憶している(図16のステップS207参照)。従って、そのような正当なPD12であるならば、秘密領域から読み出した鍵情報KT1を用いて、MC13から転送されてきたKT1 [Kc] を復号して、コンテンツ復号鍵Kcを得ることができる(ステップS222)。さらに、このコンテンツ復号鍵Kcを用いて、MC13から転送されてきた暗号化コンテンツ情報Kc [C] を復号してコンテンツCを得ることができる(ステップS223～ステップS224)。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D/A変換部12fでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

20

【0127】次に、チェックインの指示がPD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いて)、SMS2になされた場合について、図18を参照して説明する。この場合もチェックアウトの場合と同様、PD12がLCM1に対する処理をレベル0のMC13に代行して図12に示したような処理を実行することとなる。

【0128】SMS2は、デバイスID格納部4から当該LCM1のデバイスID (LCMID) を読み出し、それをPD12へ転送する(ステップS231)。

【0129】PD12では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS232)、登録されていないとき秘密領域にアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS233)。PD12は、さらに、その識別情報(PDID)を読み出して同じくLCM1へ転送する(ステップS234)。

【0130】LCM1では、PD12から転送されてきたデバイスID (PDID) をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM [PDID]) を生成する(ステップS235)。

【0131】LCM1では、この生成された情報KM [PDID] を用いて第1の相互認証処理(AKE #1)を実行し、一方、PD12でも秘密デバイスID (SPDID) を用いて第1の相互認証処理(AKE #1)を実行する(ステップS236)。

【0132】チェックインの際のステップS236の第1の相互認証処理(AKE #1)動作は、図22において、KM [MID] をKM [PDID] に置き換え、秘密メディアID (SMID) が秘密デバイスID (SPDID) に置き換えれば同様であるので、説明は省略する。

【0133】ステップS236において、LCM1とPD12との間で相互に認証されたときは、LCM1では、PD12の秘密領域(RAM領域)に格納されている鍵情報KT1を上書きするための乱数r1を従来からある乱数発生器を用いて発生して、それとMC13への上書き指示情報とをステップS236で生成した鍵情報KT (ここではKT3とする) で暗号化して(KT3 [上書き指示+r1]) PD12へ転送する(ステップS601)。なお、上書き指示には、鍵情報KT1の書き込まれているアドレスが含まれていてもよい。

【0134】PD12では、LCM1から転送されてきたKT3 [上書き指示+r1] をステップS236で生成した鍵情報KT3で復号し、乱数r1を得る(ステップS602)。この乱数r1で、PD12の秘密領域に格納されている鍵情報KT1を上書きすることで消去する(ステップS603)。

【0135】次に、鍵情報KT1が乱数r1にて確実に消去されたか否かの確認のための処理を実行する。すな

-11-

21

わち、LCM1では、ステップS235で生成された情報KM [PDID]を用いて第2の相互認証処理(AKE#2)を実行し、一方、PD12でも秘密デバイスID (SPDID)を用いて第2の相互認証処理(AKE#2)を実行する(ステップS604)。

【0136】ステップS604の第2の相互認証処理(AKE#2)は、ステップS236のAKE#1と同様であるので説明は省略する。

【0137】ステップS604において、LCM1とPD12との間で相互に認証されたときは、PD12は、鍵情報KT1が格納されていたアドレスからデータ(正常に上書きされていたれば、乱数r1)を読み取って、それをステップS604で生成された鍵情報KT(ここではKT4とする)で暗号化して(KT4[r1])LCM1へ転送する(ステップS605)。

【0138】LCM1では、PD12から転送されてきたKT4[r1]をステップS604で生成した鍵情報KT4復号し(ステップS606)、その取得されたデータとステップS601で発生した乱数r1とを比較し、一致していれば、PD12において、鍵情報KT1(あるいは、鍵情報KT1と暗号化コンテンツ情報等)が乱数r1にて消去されたと判断し、処理を終了する(ステップS607)。不一致のときはLCM1は異常を通知する等の処置を講ずるのが望ましい。

【0139】最後に、図7(c)に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該PD12の識別情報を削除する。

【0140】次に、図18とは異なる他のチェックイン時の処理動作について、図19を参照して説明する。なお、図18と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図19に示すチェックイン時の処理動作は、PD12に記録した鍵情報を消去するための指示情報(例えば、これからチェックインを行う旨の指示情報)の転送の際と、実際に消去するためのコマンド発生トリガとしての合計2回、相互認証処理(AKE)を行う点に特徴があり、ステップS236のAKE#1までの処理動作は図18と同様である。

【0141】ステップS236において、LCM1とPD12との間で相互に認証されたときは、LCM1では、これからチェックインを行う旨の指示情報をステップS236で生成した鍵情報KT(ここではKT3とする)で暗号化して(KT3[チェックイン指示])PD12へ転送する(ステップS651)。なお、チェックイン指示には、鍵情報KT1の書き込まれているアドレスが含まれていてもよい。

【0142】PD12では、LCM1から転送されてきたKT3[チェックイン指示]をステップS236で生成した鍵情報KT3で復号し、チェックイン指示情報を

(12)

特開2001-22647

22

得る(ステップS652)。

【0143】次に、実際に消去するためのコマンド発生トリガとしての第2の相互認証処理(AKE#2)を実行する(ステップS653)。ここでのAKE#2は、図23に示すように、図22のステップS308と同様に、関数gの値が一致していたか否かをチェックしたら、その結果を出力するのみである。

【0144】PD12では、関数gの値が一致している、かつ、先にチェックイン指示情報を得ていたときは、鍵情報KT1を消去する(ステップS654～ステップS655)。例えば、PD12のファイル管理領域を書き換えることにより鍵情報KT1等を消去するようにしてもよい。

【0145】最後に、図7(c)に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該PD12の識別情報を削除する。

【0146】次に、図16とは異なる他のチェックアウト時の処理動作について、図20を参照して説明する。なお、図16と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図20では、図14の場合と同様に、PD12へ転送すべきコンテンツ復号鍵Kcに対する処理に特徴がある。

【0147】図20において、LCM1では、コンテンツ復号鍵Kcに対し、まず、ステップS205で生成されたKm [PDID] (以下、これをwと表す)を用いて暗号化を施す(ステップS252)。そして、wで暗号化されたコンテンツ復号鍵Kc (w [Kc])をステップS251の相互認証処理(AKE)にて生成した鍵情報KT1を用いてさらに暗号化を行ってから(KT1[w [Kc]])、PD12へ転送する(ステップS253)。

【0148】PD12では、ステップS251の相互認証処理(AKE)にて生成した鍵情報KT1を用いて、転送されてきたKT1[w [Kc]]を復号してw [Kc]を得、これを秘密領域へ格納する(ステップS254)。

【0149】コンテンツ情報Cは、図16の場合と同様に、Kcで暗号化してから(ステップS255)、PD12を経由してMC13へ転送される(ステップS256)。

【0150】図20に示したようなチェックアウト処理動作に対応する再生処理動作について、図21を参照して説明する。なお、図20と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図21において、PD12は、自身の秘密領域に格納されている暗号化コンテンツ復号鍵w [Kc]を同じく自身の秘密デバイスID (SPDID=w)を用いて復号し、コンテンツ復号鍵Kcを得ることができる(ステップS

23

261)。このコンテンツ複号鍵Kcを用いてMC13から転送されてきた暗号化コンテンツKc[C]を復号して、コンテンツCを得ることができる(ステップS262)。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

【0151】図20に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図18、図19の説明とほぼ同様で、異なるのは、図18のステップS603、図19のステップS655でPD12の秘匿領域から消去されるのは、鍵情報KT1ではなく、w=KM[MID]で暗号化されたコンテンツ複号鍵w[Kc]であるという点である。

【0152】

【発明の効果】以上説明したように、本発明によれば、記録媒体に記録された複製コンテンツの消去が確実にしかも安全に行え、記録媒体に記録する複製コンテンツの数の管理が容易にしかも確実にできる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る記憶媒体(メディア)に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム(LCM)の構成例を示した図。

【図2】メモリ領域の構成例を示した図。

【図3】記録再生装置(PD)の内部構成例を示した図。

【図4】3種類の記憶媒体の特徴を説明するための図。

【図5】メディアインタフェース(I/F)部の内部構成例を示した図。

【図6】チェックイン後の記憶媒体の記録内容を説明するための図。

【図7】LCMの秘匿領域に格納されている密接の記憶例を示した図。

【図8】相互認証方法の概略を説明するための図。

【図9】チェックイン/チェックアウト処理手順を説明するためのフローチャートで、メディアの種類を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図10】記録媒体の種別がレベル2の場合のチェックアウト時の手順を説明するための図。

(13)

特開2001-22647

24

【図11】記録媒体の種別がレベル2の場合の再生時の手順を説明するための図。

【図12】記録媒体の種別がレベル2の場合のチェックイン時の手順を説明するための図。

【図13】記録媒体の種別がレベル2の場合のチェックイン時の他の手順を説明するための図。

【図14】記録媒体の種別がレベル2の場合のチェックアウト時の他の手順を説明するための図。

【図15】記録媒体の種別がレベル2の場合の再生時の他の手順を説明するための図。

【図16】記録媒体の種別がレベル0の場合のチェックアウト時の手順を説明するための図。

【図17】記録媒体の種別がレベル0の場合の再生時の手順を説明するための図。

【図18】記録媒体の種別がレベル0の場合のチェックイン時の手順を説明するための図。

【図19】記録媒体の種別がレベル0の場合のチェックイン時の他の手順を説明するための図。

【図20】記録媒体の種別がレベル0の場合のチェックアウト時の他の手順を説明するための図。

【図21】記録媒体の種別がレベル0の場合の再生時の他の手順を説明するための図。

【図22】相互認証処理(AKE)の処理動作について説明するための図。

【図23】相互認証処理(AKE)の他の処理動作について説明するための図。

【図24】図4(c)に示したレベル2の記録媒体の構成をより具体的に示した図。

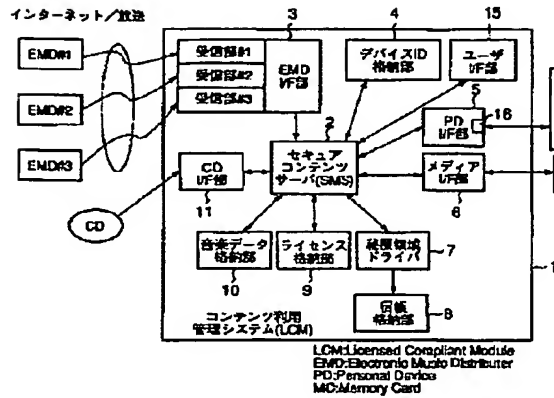
【符号の説明】

- 1…コンテンツ利用管理システム
- 2…セキュアコンテンツサーバ(SMS)
- 3…EMDインタフェース部
- 4…タイムアウト判定部
- 5…PDインタフェース(I/F)部
- 6…メディアインタフェース(I/F)部
- 7…秘匿領域ドライバ
- 8…密接格納部
- 9…ライセンス格納部
- 10…音楽データ格納部
- 11…CDインタフェース(I/F)部
- 12…記録再生装置(PD)
- 13…記憶媒体(MC)

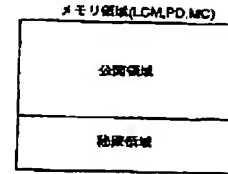
(14)

特開2001-22647

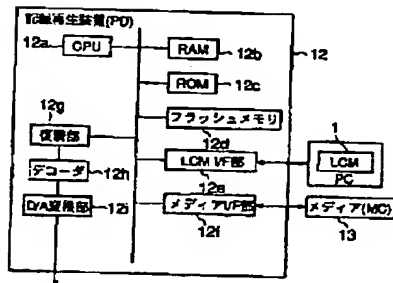
【图 1】



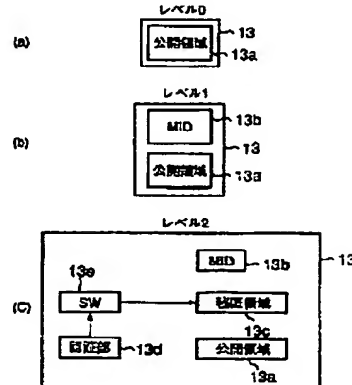
【圖 2】



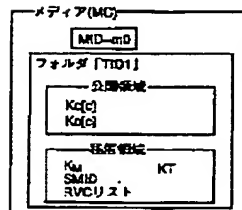
【圖3】



【圖 4】



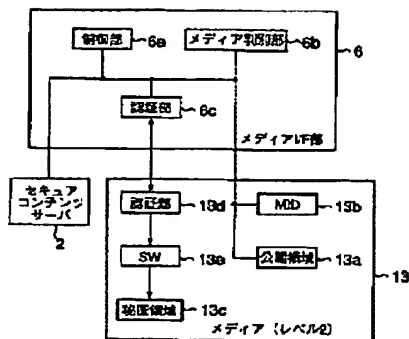
【圖6】



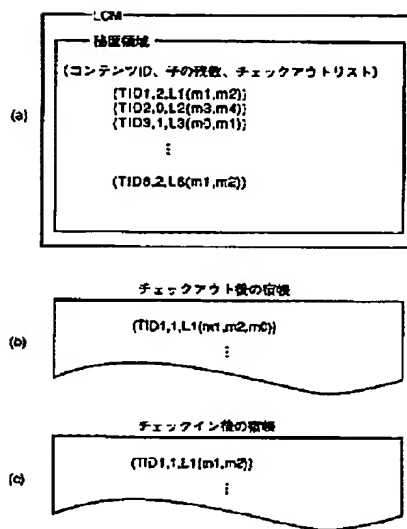
(15)

特開2001-22647

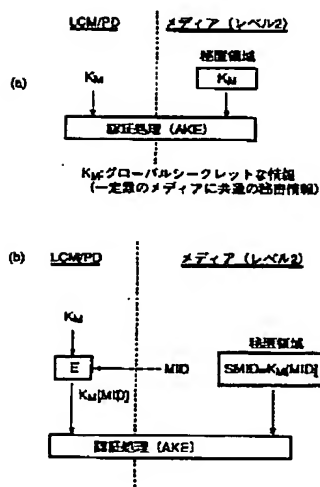
【图5】



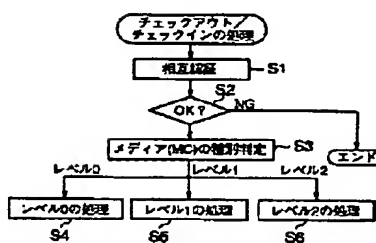
【图 7】



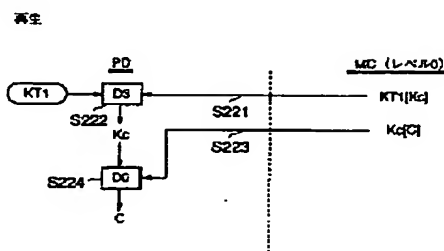
【例 8】



【例 9】



【例 17】

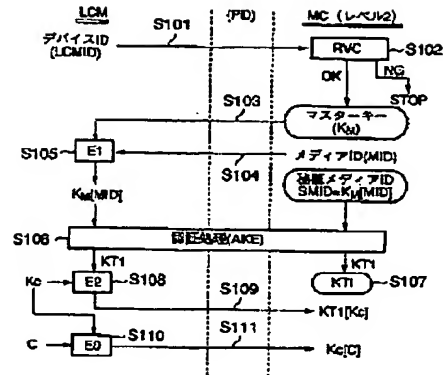


(16)

特開2001-22647

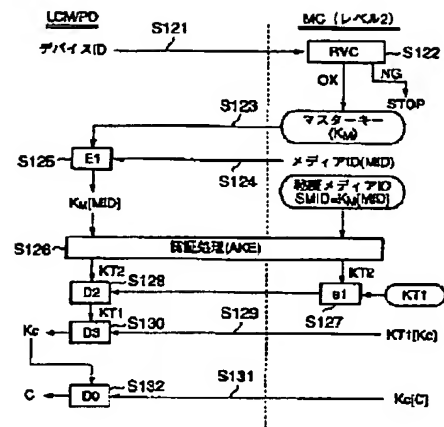
【図10】

チェックアウト



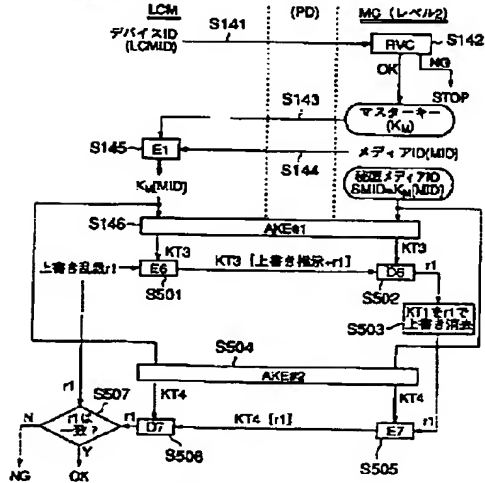
【図11】

再生



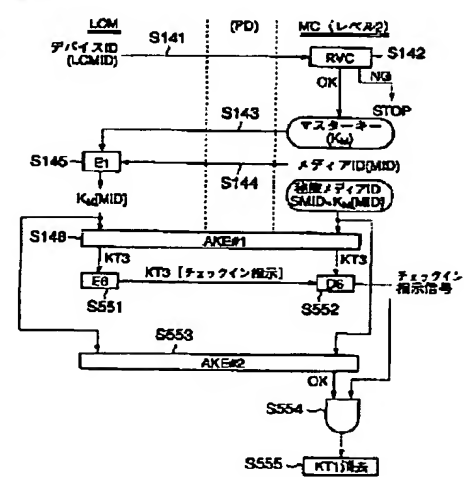
【図12】

チェックイン



【図13】

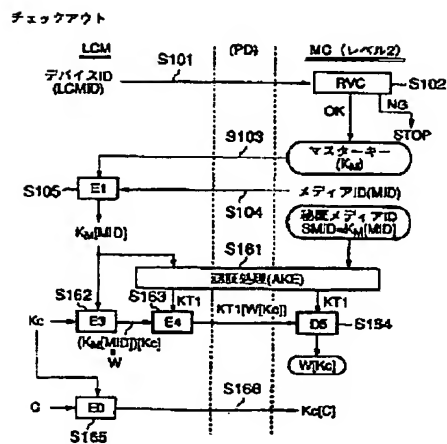
チェックイン



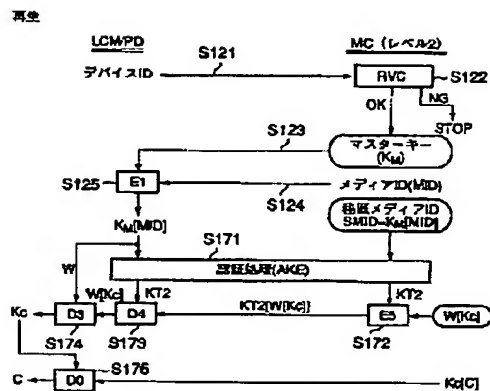
(17)

特開 2001-22647

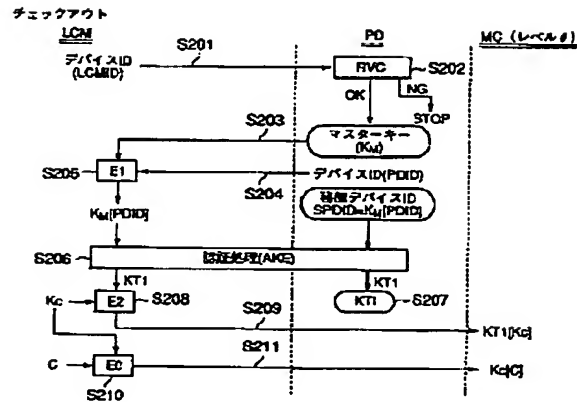
【图 14】



【圖 15】



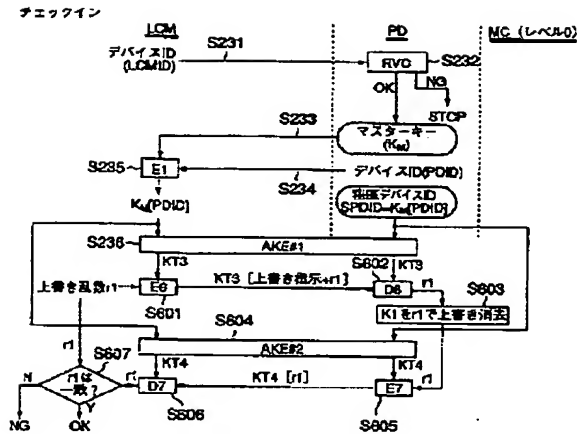
【图 1.6】



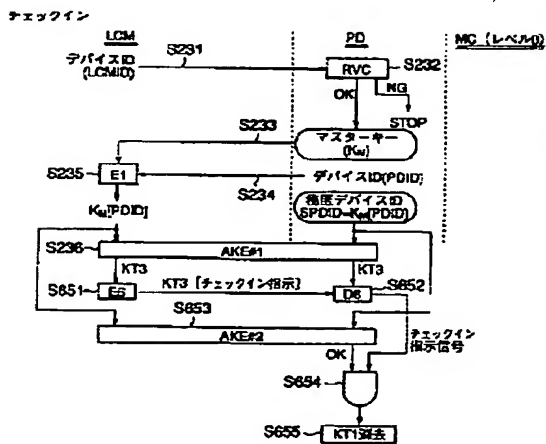
(18)

特開 2001-22647

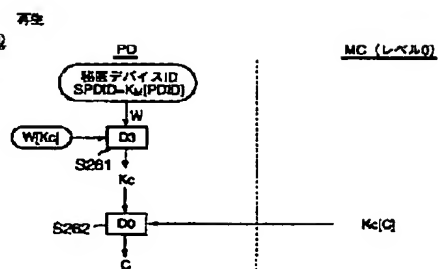
【図 18】



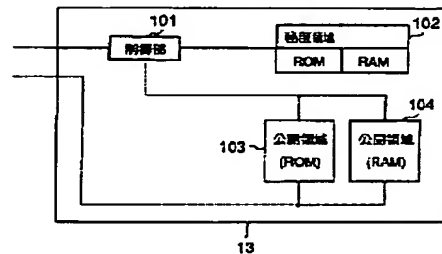
【圖 19】



【图 2 1】



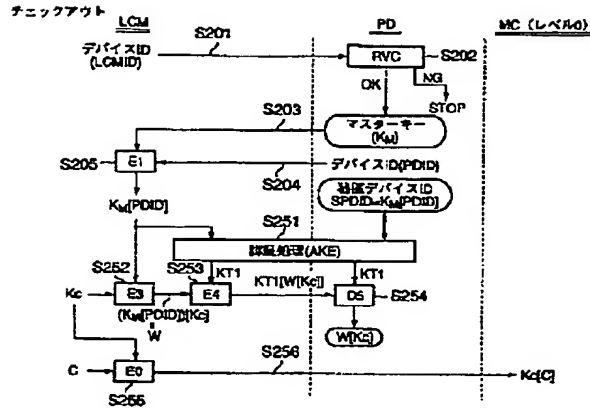
【图 2-4】



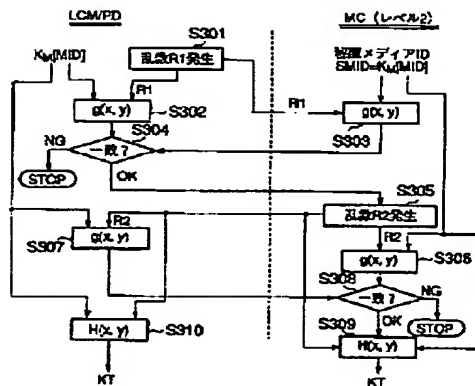
(19)

特開2001-22647

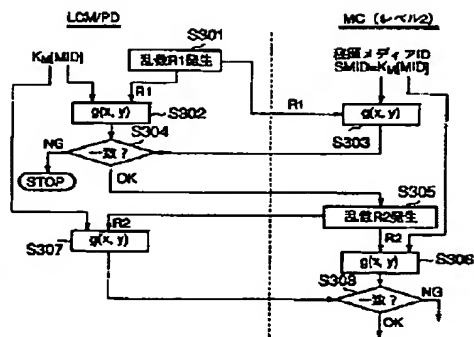
【図20】



【図22】



【図23】



フロントページの続き

(72) 発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中工場内
(72) 発明者 東間 秀之
東京都青森市末広町2丁目9番地 株式会
社東芝青森工場内
(72) 発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 原田 俊治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72) 発明者 山田 尚志
東京都港区芝浦一丁目1番1号 株式会
社東芝本社事務所内

(20)

特開 2001-22647

Fターム(参考) SB017 AA06 BA05 BA07 BA08 BB02
CA08 CA09 CA14 CA15 CA16
SB085 AE23 AE29 CA04
SD044 AB05 DE50 GK11 GK17 HL11
5J104 AA07 BA03 KA01 NA27 PA05
PA07 PA14
9A001 BB03 BB04 EE03 EE04 LL03